WHITE PAPER

Preparing for a Ransomware Attack

Executive Summary

It's 2023, and although ransomware has existed for decades, organizations still struggle with this evolving threat. In fact, based on data from our latest Fortinet 2023 Global Ransomware Report, two-thirds of organizations were targeted by ransomware and half of those fell victim to an attack. So it's not a question of "if" organizations might experience an incident, it's "when."[1] How will teams perform to get their organizations back to normal as quickly and with as little adverse impact as possible?

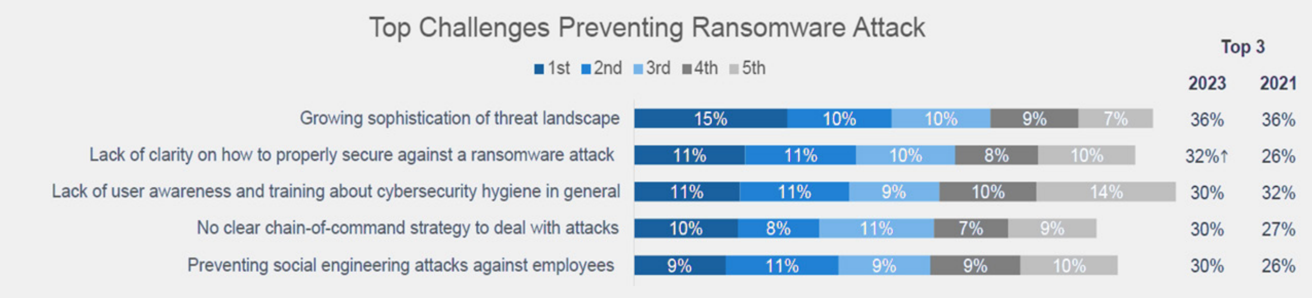
The challenge is more pronounced than ever. For instance, in the 2022 Verizon Data Breach Investigations Report, ransomware's involvement in successful breaches doubled to 25% compared to the year prior.[2] The Fortinet FortiGuard Labs threat research team closely monitors the growth in ransomware attacks. In the second half of 2022, the volume of ransomware attacks grew by 16% compared to the previous six-month period.[3] While this is unsettling, it isn't surprising: Ransomware-as-a-Service (RaaS) offers even novice cybercriminals the opportunity to easily launch sophisticated attacks for a quick payout when those attacks are successful.

Two-thirds of organizations were targeted by ransomware in the last 12 months, and 50% of those targeted fell victim to an attack.[4]

There are many actions organizations can take—from implementing the right security tools to ensuring all employees have basic cyber-hygiene knowledge—to guard against this growing threat. However, given the risk involved, organizations must have a sense of urgency and take action across technology, people, and processes. As a result, security leaders, those in the C-suite, and boards of directors must collectively prioritize ransomware risk mitigation and prevention.

Why Are Organizations Still Struggling to Guard Against Ransomware?

In the Fortinet 2023 Global Ransomware Report, we asked security leaders what they saw as the top challenges to preventing ransomware attacks. Four of the top five concerns cited were focused on processes and people, not implementing the right (or more) technologies.[5]



These concerns fall into two core areas. First, leaders are concerned about whether employees have enough cyber-hygiene knowledge to make the right decision when faced with a threat. And second, they worry that the lack of knowledge and maturity across their security team will impede their ability to protect against and respond to a ransomware attack effectively.

Recommendations for Security Teams

There are many actions organizations can and should take to defend against ransomware that will help alleviate the challenges cited above. To effectively mitigate ransomware:

Assess your people, processes, and technologies

- Perform a ransomware preparedness assessment to assess the overall readiness of your security team's people, processes, and tools to effectively prevent, rapidly detect, and respond to a ransomware attack.
- Consider engaging a third-party advisor like Fortinet for an independent assessment to help you garner more consideration and support among leadership for making enhancements to your security program.
- Security leaders should reassess staffing levels and existing expertise to ensure teams have the right staff members and skill sets to mitigate a ransomware incident effectively.

Incorporate ransomware into your incident response plan

- Create, maintain, and periodically test and update an incident response (IR) plan specifically focused on countering a ransomware threat.
- For an expert evaluation of an IR plan, consider a review with a third party. Vendors like Fortinet provide an objective assessment and can offer guidance and recommendations for improving your organization's plan.

Prioritize ransomware prevention and mitigation across the organization

- Elevate the ransomware issue within your organization to C-level executives and the board of directors. Organizations that consider ransomware mitigation their most important priority fall victim to ransomware less than organizations that consider mitigation a top three priority (52% versus 43%, respectively).[6]
- Establish and foster two-way communication with the C-suite and board of directors on cybersecurity-related things.
- Include the organization's leadership in your IR plan, especially regarding the escalation and crisis decision-making phases.

Implement the right tools

- Implement, optimize, or plan to adopt the seven most-cited technologies to aid in preventing a ransomware incident:

1. Internet-of-Things (IoT) protection
2. Next-Generation Firewalls (NGFWs)
3. Secure access service edge (SASE) solutions
4. Cloud workload protection (CWP)
5. Endpoint detection and response (EDR)
6. Zero-trust network access (ZTNA) principles, policies, and tools
7. Secure email gateways (SEGs)

Sixty-two percent of survey respondents cited IoT security as essential to securing their organization against ransomware (versus 49% who said the same in our 2021 report).[7] It's clear IoT's proliferation and the risk it poses to organizations is more pronounced than ever. As a result, security teams should be aggressive in seeking approaches to help discover, profile, and secure IoT devices to prevent their use in ransomware and other attacks.

Security teams should also have robust backup procedures and solutions that ransomware attacks can't compromise. These must be regularly tested to ensure that data can be recovered as rapidly and reliably as possible.

Train security personnel

- On-the-job training during a ransomware incident is not the time for security teams to effectively learn how to mitigate and respond to a ransomware threat. Organizations should consider tabletop exercises, specifically designed for ransomware scenarios, to educate and prepare staff for how best to approach incidents in the future.
- Fund training through the SANS Institute, Information Systems Audit and Control Association (ISACA), Cloud Security Alliance, and other associations or organizations. In addition, encourage your staff to take advantage of free training provided by vendors like Fortinet on a variety of cybersecurity topics.

Address the risks posed by employees

Get serious about security awareness training and its overall efficacy in changing employee behavior so that everyone can play a role in enhancing the organization's security posture.

- Evaluate the efficacy of any existing security awareness training programs. Is the program simply meant to check a compliance or regulatory box, or is it designed to change employee behavior, improve the organization's overall security posture, and reduce risk?

- Consider increasing the hours the security teams spend on educating employees, as it's likely that many organizations don't devote enough resources to these efforts. Changing behavior is difficult, especially when the effort is under-resourced. However, cyber knowledge is more crucial than ever, given the use of RaaS and technologies driven by artificial intelligence (AI) that attackers can exploit.
- Keep in mind that every employee needs to be even more knowledgeable than ever to be effective in spotting, avoiding, and reporting potential threats. This includes educating and testing employees on several critical areas:
  - Cybersecurity principles and why cybersecurity is so important
  - Psychological approaches fraudsters and attackers use, such as bias, urgency, and social engineering
  - Psychological principles employees should use when faced with potential threats, such as thinking the scenario through before acting or considering the context of the situation
  - Current, real-world examples of threats perpetrated against employees
  - How threat actors may use a multi-channel approach when targeting employees
  - How AI is being used by threat actors and changing the caliber of threats
- Incorporate testing employees using real-world threats and scenarios, including social engineering. Education programs must be rigorous in educating employees, including testing through phishing, vishing, and smishing simulations. Ask your current vendor how they address concerns that emerging AI tools enable attackers to launch more complex and convincing threats targeting employees.

Of those organizations that fell victim to ransomware, 70% paid the requested ransom.[8]

Ransomware Is Rampant, but Fortinet Can Help

Ransomware presents tremendous risk to organizations, ranging from the loss of sensitive data to significant disruption of operations. The Fortinet Security Fabric, with solutions powered by machine learning and AI, enables you to deploy integrated prevention, detection, and response capabilities to protect your enterprise against ransomware attacks throughout the entire life cycle or kill chain, helping you to mitigate ransomware risk effectively. In addition, Fortinet provides security teams with services to assess operational readiness and train team members in effectively responding to a ransomware incident.

[1] "The 2023 Global Ransomware Report," Fortinet, April 24, 2023.

[2] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.

[3] "FortiGuard Labs 2H 2022 Threat Landscape Report," Fortinet, February 22, 2023.

[4] "The 2023 Global Ransomware Report," Fortinet, April 24, 2023.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

May 23, 2023 5:57 PM
2144637-0-0-EN